Ph.D. Title Proposal

on

A Framework for Enhancing Educational System Security through Honeypot Integration

Submitted in partial fulfillment of the
requirement for the award of the Degree of

Doctor of Philosophy

in

Information Technology

by

Mr. Pankaj Vijay Meheshre

under the guidance of

Dr. Nilakshi S. Jain

Department of Information Technology

Mahavir Education Trust's

Shah and Anchor Kutchhi Engineering College

Chembur, Mumbai-400088

University of Mumbai

January 2025

THE TOPIC APPROVAL REPORT TO BE SUBMITTED TO THE UNIVERSITY OF MUMBAI FOR THE DEGREE OF **Ph.D. (SCIENCE AND TECHNOLOGY)** IN THE SUBJECT OF **INFORMATION TECHNOLOGY**

Title of Topic	:	A Framework for Enhancing Educational System Security through Honeypot Integration
Name of the Student	:	Pankaj Vijay Meheshre
Basic Qualification	:	M. E. (Computer Engineering) B.E. (Computer Science & Engineering)
In the Case of Ph.D. student Year of Passing of PET/NET/SET/GATE (Teaching Experience)	:	PET-2022
Name of the Research Supervisor/ Guide	:	Dr. Nilakshi S. Jain
Date of Superannuation / Retirement	:	07/10/2046
Name of the Research Center	:	Shah and Anchor Kutchhi Engineering College
Signature of Student	:	
Signature of the Research Supervisor	:	

Shah & Anchor Kutchhi Engg. College ★ Autonomous Institute Mumbai

Head / Director / Principal
Research Centre
Dr. Bhavesh Patel
Principal
Shah & Anchor Kutchhi Engg. College
Waman Tukaram Patil Marg,
Next to Dukes Co., Chembur,
Mumbai - 400 088.

Sr. no.	Content	Page no.
1	Introduction	1
2	Literature Review	4
3	Research Gap	8
4	Problem Statement	9
5	Objectives of Study	10
6	Research Hypothesis	10
7	Research Methodology	10
8	Expected Outcomes	11
9	References	13

Statement by the Candidate

I wish to state that the work embodied in this synopsis titled "A Framework for Enhancing Educational System Security through Honeypot Integration" forms my own contribution to the work carried out under the guidance of Dr. Nilakshi S. Jain at the Shah and Anchor Kutchhi Engineering College. I declare that this written submission represents my ideas in my own words and where others ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

Name: **Mr. Pankaj Vijay Meheshre**

Roll Number: **124PHIT1002**

Abstract

Indian higher education institutions face mounting cybersecurity threats, endangering sensitive academic data. This research proposes a comprehensive framework for investigating these challenges, focusing on vulnerabilities, current security practices, and the potential of honeypots in enhancing data protection. The framework incorporates a mixed-methods approach, combining a thorough literature review, analysis of recent cyberattack case studies, and semi-structured interviews with IT professionals and security experts from Indian universities. The analysis of qualitative data and synthesis of quantitative findings reveal key challenges, including decentralized IT systems, limited cybersecurity awareness, and increasingly sophisticated attack techniques. The framework also evaluates existing cybersecurity practices and strategies, identifying strengths, weaknesses, and areas for improvement. Furthermore, it explores the strategic role of honeypots in strengthening cybersecurity, examining their benefits, challenges, and best practices for implementation within the higher education context. The proposed framework provides a structured approach for assessing vulnerabilities, evaluating current practices, and developing targeted mitigation strategies, including the strategic deployment of honeypots, to protect sensitive academic data in Indian higher education institutions. The findings offer valuable insights for policymakers, administrators, and IT professionals, enabling them to create and implement effective cybersecurity strategies to counter evolving threats and safeguard academic data.

Keywords: Cybersecurity, Higher Education, India, Honeypots, Cyberattacks, Vulnerabilities.

1. Introduction

The proliferation of technology in the education sector has brought numerous benefits, such as improved accessibility, enhanced learning experiences, and increased collaboration. However, this reliance on digital infrastructure has also exposed academia to a myriad of cybersecurity threats. Indian higher education institutions, with their extensive data repositories and complex network environments, are particularly vulnerable to these challenges. [1]

Emerging Cybersecurity Threats in Indian Higher Education

Indian higher education institutions are facing a growing array of cybersecurity threats, ranging from malware attacks to data breaches and intellectual property theft [1] [2] [3]. Institutions in India have been targeted by cyber-attacks, with over 300 universities worldwide affected in a single incident in 2018, compromising more than 100,000 professors' email accounts and exposing 31 terabytes of valuable data. [1] The pandemic-induced shift to online learning has further exacerbated these vulnerabilities, as the increased use of remote access and cloud-based platforms has opened new avenues for malicious actors to exploit. [3]

Additionally, the inherent openness of university networks and the wide range of user motivations and devices accessing the system make Indian higher education institutions prime targets for cyber threats. Incidents such as the data breach at Arden University in 2022, where almost 44,000 student records were obtained due to human errors, highlight the severity of the challenge. [3]

Factors Influencing Cybersecurity Challenges

Several key factors contribute to the cybersecurity challenges faced by Indian higher education institutions. The rapid expansion of the Indian higher education system, with 21,825 colleges and 911 universities, has led to an increased reliance on e-governance applications, which can introduce vulnerabilities if not properly secured [1]. Moreover, the lack of awareness and understanding of data security among the academic community, as well as the insufficient implementation of appropriate security controls, have exacerbated the risk of data breaches and cyber attacks. [2]

Strategies for Enhancing Cybersecurity in Indian Higher Education

To address the cybersecurity challenges in Indian higher education, a multifaceted approach is necessary. Enhanced security awareness and training programs for students, faculty, and administrative staff can help mitigate the risk posed by human errors and insider threats. Implementing robust access controls, regularly updating software and systems, and deploying advanced threat detection and response mechanisms can also strengthen the overall cybersecurity posture of Indian higher education institutions. [3] [1]

Additionally, the adoption of cutting-edge technologies, such as artificial intelligence and machine learning, can help institutions detect and respond to cyber threats more effectively.

Collaboration between academia, industry, and government agencies is also crucial in developing comprehensive cybersecurity strategies and sharing best practices to protect the sensitive data and intellectual property of Indian higher education institutions.

The rapid digitalization of Indian higher education, while offering numerous benefits, has simultaneously exposed the sector to a growing array of cybersecurity threats. These threats compromise sensitive academic and personal data, undermining the integrity of academic research, student privacy, and institutional reputation. This investigation goes into the specific cybersecurity challenges faced by Indian higher education institutions in protecting this valuable data, with a particular focus on the potential of honeypots as a security measure. Honeypots are decoy systems designed to attract and trap cybercriminals, providing valuable insights into their tactics and techniques [4]. They can be categorized into various types, including low-interaction honeypots, which mimic basic services and capture limited information, and high-interaction honeypots, which simulate real systems with greater complexity and capture more detailed data [5]. By deploying honeypots, universities can proactively detect and analyze cyber threats, gather intelligence on attack patterns, and strengthen their overall security posture [6]. This research will examine the vulnerabilities inherent in the expanding digital infrastructure, the evolving tactics of cybercriminals targeting the sector, and the awareness and preparedness levels within the Indian academic community, while also exploring the role of honeypots in mitigating these challenges. By exploring these critical aspects, this study aims to provide insights into

the current cybersecurity landscape of Indian higher education and propose potential strategies for strengthening data protection measures.

Honeypots: A Proactive Defense for Academic and Personal Data

Honeypots play a crucial role in protecting academic and personal data by acting as decoys to lure and trap cyberattackers, diverting them from actual targets and providing valuable insights into their tactics, techniques, and procedures [4]. They offer a proactive defense mechanism, allowing institutions to detect and analyze threats in a controlled environment before they can compromise sensitive information. Within the context of higher education, honeypots can be instrumental in safeguarding research data, student records, intellectual property, and other critical assets.

Types of Honeypots

Honeypots can be classified into various types based on their level of interaction and complexity:

- **Low-Interaction Honeypots:** These honeypots emulate basic services and capture limited information about attackers. They are relatively easy to deploy and maintain, posing minimal risk of compromise [7].
- **High-Interaction Honeypots:** These honeypots simulate real systems with greater complexity, allowing for more in-depth analysis of attacker behavior. They can capture more detailed data, but also carry a higher risk of compromise if not properly secured [8].
- **Pure Honeypots:** These honeypots are dedicated systems solely designed for attracting and trapping attackers. They do not host any real services or data.
- **Production Honeypots:** These honeypots are integrated into existing production systems, making them more difficult for attackers to distinguish from legitimate targets.

Honeypot Frameworks and Applications

Several frameworks and applications facilitate the deployment and management of honeypots:

- **Honeyd:** This popular open-source framework allows for the creation of virtual honeypots that can simulate various operating systems and services [9].

- **Kippo:** This high-interaction honeypot specifically targets SSH servers, capturing keystrokes and commands executed by attackers.

The application of honeypots in higher education can be diverse:

- **Early Warning System:** Honeypots can serve as an early warning system, alerting institutions to potential attacks and providing valuable time to implement countermeasures [6].
- **Threat Intelligence Gathering:** By analyzing the data captured by honeypots, institutions can gain insights into attacker tactics, techniques, and procedures, enabling them to develop more effective security strategies [10].
- **Malware Analysis:** Honeypots can be used to capture and analyze malware samples, providing valuable information about their functionality and potential impact.
- **Security Awareness Training:** Honeypots can be incorporated into cybersecurity training programs to provide students and staff with practical experience in identifying and responding to cyber threats [11].

By strategically deploying and managing honeypots, Indian higher education institutions can significantly enhance their cybersecurity posture and protect valuable academic and personal data from evolving cyber threats [12].

2. Literature Review

This research will begin with an extensive literature review to understand the current state of honeypot technology and its applications in the context of higher education.

1 **Honeypots: Tracking Hackers:** Spitzner [4] provides a foundational understanding of honeypots and their use in tracking hackers. *Limitation:* Being an older resource, it may not fully reflect the current threat landscape and advancements in honeypot technology.

2 **A Survey on Honeypot Software and Data Analysis:** Nawrocki et al. [5] provide a survey of honeypot software and data analysis techniques, offering practical guidance for implementing and managing honeypots. *Limitation:* The

paper focuses on technical aspects and lacks discussion on the strategic implications of honeypot deployment in academic settings.

3 **Cyber Security System With SIEM And Honeypot In Higher Education:** Suroso and Prastya [6] discuss the implementation of a cybersecurity system combining SIEM and honeypots in higher education. They highlight the importance of real-time threat monitoring and response. *Limitation:* The paper lacks detailed analysis of the honeypot's effectiveness and its specific contribution to overall security.

4 **Deployment of a low interaction honeypot in an organizational private network:** Chamotra et al. [7] present a case study of deploying a low-interaction honeypot in an organizational network. They discuss the benefits and challenges of using honeypots for internal threat detection. *Limitation:* The study's focus is on organizational networks and not specifically tailored to the higher education context.

5 **A Highly Interactive Honeypot-Based Approach to Network Threat Management:** Yang et al. [8] propose a highly interactive honeypot-based approach for network threat management. They emphasize the importance of real-time threat detection and response. *Limitation:* The paper's focus is on general network threat management and not specifically tailored to the unique challenges of higher education.

6 **A Survey: Recent Advances and Future Trends in Honeypot Research (n.d.):** Bringer et al. [9] present a comprehensive survey of honeypot research, categorizing advancements into new honeypot types, data utilization, configuration, counter-detection, and legal/ethical issues. They emphasize the importance of adapting honeypots to evolving networking environments and user behavior. *Limitation:* The survey lacks specific examples of honeypot deployment in academic settings.

7 **An Overview of Honeypot Systems:** Titarmare et al. [10] provide an overview of honeypot systems, discussing their various types, advantages, and disadvantages. They also touch upon the concepts of honeynets and honeywalls. *Limitation:* The paper offers a general overview and lacks a focus on specific applications in higher education.

8 **Benefits of Honeypots in Education Sector:** Ahmad et al. [11] discuss the advantages of using honeypots in educational settings to enhance network security and provide real-time security education for students. They highlight the ability of honeypots to capture and analyze attacks, acting as early warning sensors. *Limitation:* The paper primarily focuses on awareness and lacks in-depth technical analysis.

9 **Cyber-Security Awareness In India: How Much Students Of Higher Education Are Aware? (n.d.):** Kant [12] explores cybersecurity awareness among Indian higher education students, examining their knowledge of cyber threats and protective measures. The study highlights the need for improved awareness and education to mitigate risks. *Limitation:* The study focuses on awareness and doesn't delve into specific security solutions like honeypots.

10 **A Study Of Factors Influencing Cyberattacks:** Ikuomenisan [15] examines the factors influencing cyberattacks, providing insights into attacker motivations and vulnerabilities. *Limitation:* The study doesn't directly address the role of honeypots in mitigating these attacks.

11 **A survey of network-based intrusion detection data sets:** Ring et al. [16] present a survey of network-based intrusion detection datasets, which can be valuable for training and evaluating honeypot systems. *Limitation:* The paper focuses on datasets and not on honeypot deployment strategies.

12 **A comprehensive survey on cyber deception techniques to improve honeypot performance:** Javadpour et al. [17] discuss various cyber deception techniques to enhance honeypot performance, including methods for attracting attackers and increasing the realism of honeypots. *Limitation:* The survey is broad and doesn't specifically address the application of these techniques in higher education.

13 **A Detailed Analysis of Benchmark Datasets for Network Intrusion Detection System:** Ghurab et al. [18] analyze benchmark datasets for network intrusion detection systems, which can be relevant for evaluating the effectiveness of honeypots. *Limitation:* The paper's focus is on datasets and not specifically on honeypot applications in higher education.

14 **HoneyTrack: An improved honeypot:** Auti et al. [19] propose HoneyTrack, an improved honeypot system designed for enhanced threat detection and analysis. They emphasize the importance of real-time monitoring and data visualization. *Limitation:* The paper focuses on the technical aspects of HoneyTrack and lacks discussion on its practical application in higher education.

15 **Exploring Cybersecurity Awareness and Training Strategies To Protect Information Systems and Data:** Hanna [20] explores cybersecurity awareness and training strategies for protecting information systems and data. *Limitation:* The paper focuses on general cybersecurity awareness and doesn't specifically address the role of honeypots.

16 **Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political:** Gandhi et al. [21] examine the various dimensions of cyberattacks, including cultural, social, economic, and political aspects. *Limitation:* The paper provides a broad overview of cyberattacks and doesn't delve into specific mitigation techniques like honeypots.

17 **Towards Sustainable E-Learning Platforms in the Context of Cybersecurity: A TAM-Driven Approach:** Alquran [22] investigates sustainable e-learning platforms in the context of cybersecurity using a TAM-driven approach. *Limitation:* The paper focuses on e-learning platform security and doesn't specifically address the use of honeypots.

18 **Systematic Review of Graphical Visual Methods in Honeypot Attack Data Analysis:** Ikuomenisan and Morgan [23] present a systematic review of graphical visual methods used in honeypot attack data analysis. They highlight the importance of effective data visualization for understanding attack patterns. *Limitation:* The paper focuses on data analysis techniques and not on the strategic deployment of honeypots.

19 **Honeypot-Based Security Enhancements For Information Systems:** Franco [24] discusses honeypot-based security enhancements for information systems, emphasizing their role in threat detection and data collection. *Limitation:* The paper provides a general overview and lacks specific examples of honeypot implementation in higher education.

20 **Visualization of Misuse-Based Intrusion Detection: Application to Honeynet Data:** Zurutuza et al. [25] explore the visualization of misuse-based intrusion detection using honeynet data. They emphasize the importance of visualizing attack patterns for improved understanding and response. *Limitation:* The paper focuses on data visualization techniques and not on the strategic deployment of honeypots in higher education.

21 **Deploying a University Honeypot: A case study:** Mahmoud and Pedersen [26] analyze the deployment of a honeypot within a university setting, examining its effectiveness in gathering information about real-world attacks targeting universities. They discuss the selection and deployment process, as well as the results obtained. *Limitation:* The case study is limited to a specific university environment and may not be generalizable to all higher education institutions.

22 **Meta-Review of Recent and Landmark Honeypot Research and Surveys:** Ikuomenisan and Morgan [27] conduct a meta-review of honeypot research and surveys, identifying key themes and trends in the field. They highlight the growing interest in honeypots and the need for more systematic research methodologies. *Limitation:* The meta-review focuses on general honeypot research and lacks specific insights into applications within higher education.

3. Research Gap

- Research on cybersecurity in educational institutions shows several gaps in addressing the full range of security challenges faced by these systems. Many studies, like *The Security Ambiguity and Vulnerability in G2C eGovernance System*, focus too narrowly on specific threats like cyberattacks, without considering the broader security needs of educational institutions. Similarly, research such as *The Understanding Cyber Threats Against the Universities, Colleges, and Schools* highlights the importance of awareness but lacks practical solutions for mitigating cybersecurity risks in schools and universities.
- Additionally, some studies, including *The Data Security Crisis in Universities* and *The Honeypots: Tracking Hackers*, do not provide updated or

comprehensive strategies. For example, *The Data Security Crisis in Universities* fails to offer a clear plan for preventing data breaches, while *The Honeypots: Tracking Hackers* is outdated and does not address the latest cybersecurity challenges. Research like *The Cyber Security System With SIEM and Honeypot in Higher Education* focuses mainly on technical tools but does not consider how to apply them effectively within the educational sector.

- Lastly, many studies overlook the practical use of honeypots in educational settings. For instance, *The Cyber Threat Analysis for University Networks via Virtual Honeypots* and *The A Survey: Recent Advances and Future Trends in Honeypot Research* do not explore the specific challenges of deploying honeypots in schools and universities. Research like *The Benefits of Honeypots in Education Sector* focuses more on spreading awareness than on exploring how honeypots can be effectively implemented in the education sector. These gaps make it difficult to create a comprehensive cybersecurity plan for educational institutions that fully integrates honeypots and other advanced security measures.

4. Problem Statement

Academic institutions are increasingly vulnerable to cyber threats, yet traditional security measures often fail to effectively detect and mitigate these risks. Honeypots, which are designed to attract and study cyber attackers, offer a promising solution but remain underutilized in educational settings. This research aims to develop a comprehensive framework for integrating honeypots into the cybersecurity systems of academic institutions, analyze their effectiveness, and create a cybersecurity policy to enhance threat detection and mitigation. The framework will be validated through real-world deployment, aiming to improve the overall security posture of educational institutions.

5. Objectives of Study

- ➢ Analyze current literature on the cybersecurity landscape within the academic institute.
- ➢ Deploy and implement various types of honeypots to detect and mitigate cyber threats in academic institute, and analyze their strengths and weaknesses while generating relevant datasets.
- ➢ Develop a framework and cyber security policy to enhance the detection and mitigation of cyber threats in academic institute.
- ➢ Validate the proposed framework through deployment in a real academic setting.

6. Research Hypothesis

H1: There is an acute need to design a system that enhances the detection and mitigation of cyber threats in academic institutions.

H2: Implementing honeypots in academic institute improves the detection and mitigation of cyber threats.

7. Research Methodology

The research methodology section will outline the research approach, data collection methods, analysis techniques used in this study. The methodology is structured into different phases explained below and shown in figure 1.

This research methodology section will outline the step-by-step process of research methodology. Each block represents a major phase of the research, starting with literature review and analysis, followed by honeypot deployment, framework development, real-world validation, and finally, conclusion and recommendations shown in figure 1.

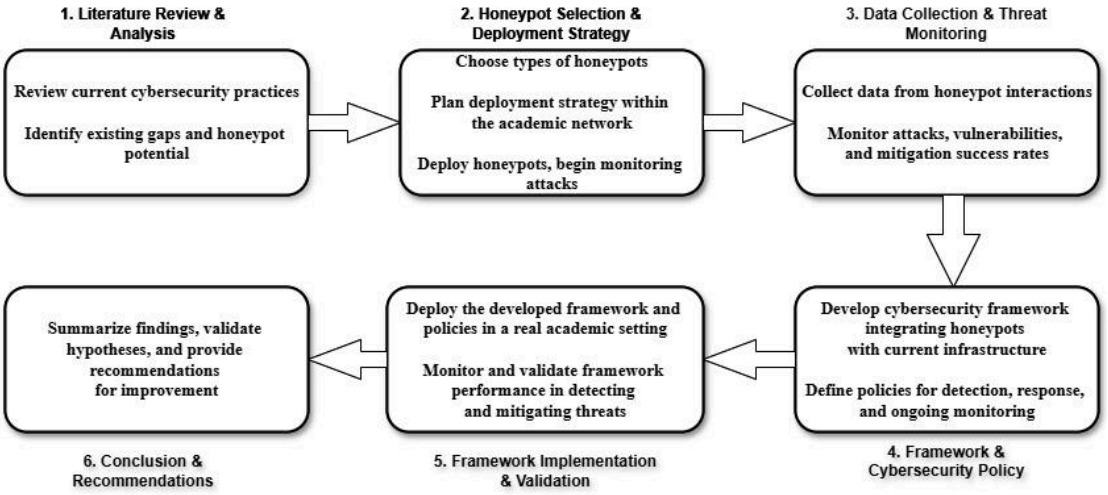
1. Literature Review & Analysis
Review current cybersecurity practices
Identify existing gaps and honeypot potential
2. Honeypot Selection & Deployment Strategy
Choose types of honeypots
Plan deployment strategy within the academic network
Deploy honeypots, begin monitoring attacks
3. Data Collection & Threat Monitoring
Collect data from honeypot interactions
Monitor attacks, vulnerabilities, and mitigation success rates
4. Framework & Cybersecurity Policy
Develop cybersecurity framework integrating honeypots with current infrastructure
Define policies for detection, response, and ongoing monitoring
5. Framework Implementation & Validation
Deploy the developed framework and policies in a real academic setting
Monitor and validate framework performance in detecting and mitigating threats
6. Conclusion & Recommendations
Summarize findings, validate hypotheses, and provide recommendations for improvement

Figure 1. Phases in the methodology for honeypots in academic institute

1. **Literature Review & Research Setup**: Review the cybersecurity landscape, identify gaps, and set up research hypotheses.
2. **Honeypot Selection & Deployment**: Choose appropriate honeypot types and deploy them within the academic institution's network.
3. **Data Collection & Threat Monitoring**: Gather data from honeypots and monitor cyber threats to assess the system's performance.
4. **Framework & Cybersecurity Policy**: Develop a comprehensive framework integrating honeypots and cybersecurity policies for incident management and threat detection.
5. **Framework Implementation & Validation**: Implement the framework in a real-world academic setting and validate its performance.
6. **Conclusion & Recommendations**: Validate hypotheses, and provide conclusions and recommendations for future improvements.

8. Expected Outcomes

The proposed study is expected to yield the following outcomes:

Understanding Cybersecurity Landscape in Academic Institutions

- Analysis of existing cybersecurity measures and vulnerabilities in academic institutions, highlighting gaps that honeypots can address.

Data on Honeypot Effectiveness

- Collection and analysis of data from different types of honeypots (low, high, hybrid) to assess their effectiveness in detecting and mitigating cyber threats.

Development of Cybersecurity Framework and Policies

- Creation of a cybersecurity framework integrating honeypots with existing measures, including policies for detection, response, and threat mitigation.

Real-World Framework Validation

- Deployment of the developed framework in an academic setting to validate its performance in enhancing cybersecurity and reducing successful cyberattacks.

Improved Threat Detection and Mitigation

- Demonstration of improved threat detection, faster response times, and better overall cybersecurity through honeypot integration.

Contribution to Cybersecurity Best Practices

- Provision of a practical framework and recommendations for other academic institutions, contributing to the broader field of cybersecurity in educational settings.

References

[1] S. Gill, “Security ambiguity and vulnerability in G2C eGovernance system: Empirical evidence from Indian higher education,” Sep. 12, 2020, Indian Society for Education and Environment. doi: 10.17485/ijst/v13i34.1373.

[2] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, “Understanding Cyber Threats Against the Universities, Colleges, and Schools,” Jan. 01, 2023, Cornell University. doi: 10.48550/arxiv.2307.07755.

[3] L. Jin, W. Xiao, and C. Zhang, “Data security crisis in universities: identification of key factors affecting data breach incidents,” May 30, 2023, Palgrave Macmillan. doi: 10.1057/s41599-023-01757-0.

[4] L. Spitzner, Honeypots: Tracking Hackers. 2002.

[5] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, “A Survey on Honeypot Software and Data Analysis,” Jan. 01, 2016, Cornell University.

[6] J. S. Suroso and C. P. Prastya, “Cyber Security System With SIEM And Honeypot In Higher Education,” Jun. 01, 2020, IOP Publishing.

[7] S. Chamotra, J. S. Bhatia, R. Kamal, and A. K. Ramani, “Deployment of a low interaction honeypot in an organizational private network,” Apr. 01, 2011.

[8] X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, and J. Zhao, “A Highly Interactive Honeypot-Based Approach to Network Threat Management,” Mar. 28, 2023, Multidisciplinary Digital Publishing Institute.

[9] M. L. Bringer, C. Chelmecki, and H. Fujinoki, “A Survey: Recent Advances and Future Trends in Honeypot Research,” Sep. 01, 2012.

[10] N. Titarmare, N. Hargule, and A. Gupta, “An Overview of Honeypot Systems,” Feb. 28, 2019, ISROSET.

[11] A. Ahmad, M. Ali, J. Mustafa, S. Arabia, and S. Arabi, “Benefits of Honeypots in Education Sector,” Jan. 01, 2011.

[12] R. Kant, “Cyber-Security Awareness In India: How Much Students Of Higher Education Are Aware?” Jun. 2023.

[13] W. Davis and H. Chi, “Cyber threat analysis for university networks via virtual honeypots,” Mar. 24, 2011. doi: 10.1145/2016039.2016144.

[14] J. Zhai and K. Wang, “Research on applications of honeypot in Campus Network security,” May 01, 2012. doi: 10.1109/mic.2012.6273260.

[15] G. T. Ikuomenisan, “A Study Of Factors Influencing Cyberattacks.” Dec. 2022.

[16] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network-based intrusion detection data sets,” Jun. 11, 2019, Elsevier BV.

[17] A. Javadpour, F. Ja’fari, T. Taleb, M. Shojafar, and C. Benzaïd, “A comprehensive survey on cyber deception techniques to improve honeypot performance,” Mar. 01, 2024, Elsevier BV.

[18] M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, and S. M. Othman, “A Detailed Analysis of Benchmark Datasets for Network Intrusion Detection System,” Apr. 14, 2021.

[19] A. Auti, S. Pagar, V. Mishra, J. Makwana, and S. Borade, “HoneyTrack: An improved honeypot,” Feb. 18, 2023.

[20] M. Hanna, “Exploring Cybersecurity Awareness and Training Strategies To Protect Information Systems and Data,” Jan. 01, 2020.

[21] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. A. Laplante, “Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political,” Jan. 01, 2011, Institute of Electrical and Electronics Engineers.

[22] H. Alquran, “Towards Sustainable E-Learning Platforms in the Context of Cybersecurity: A TAM-Driven Approach.” Jun. 13, 2023.

[23] G. Ikuomenisan and Y. Morgan, “Systematic Review of Graphical Visual Methods in Honeypot Attack Data Analysis,” Jan. 01, 2022, Scientific Research Publishing.

[24] J. R. Franco, “Honeypot-Based Security Enhancements For Information Systems.” Jun. 14, 2022.

[25] U. Zurutuza, E. Ezpeleta, Á. Herrero, and E. Corchado, “Visualization of Misuse-Based Intrusion Detection: Application to Honeynet Data,” Springer Science+Business Media, 2011, p. 561.

[26] R. V. Mahmoud and J. M. Pedersen, “Deploying a University Honeypot: A case study,” Sep. 01, 2019.

[27] G. Ikuomenisan and Y. Morgan, “Meta-Review of Recent and Landmark Honeypot Research and Surveys,” Jan. 01, 2022, Scientific Research Publishing.

[28] T. Sethi and R. Mathew, “A Study on Advancement in Honeypot based Network Security Model,” Feb. 04, 2021. doi: 10.1109/icicv50876.2021.9388412.

[29] J. Z. Guizhou and Z. Liu, “New honeypot system and its application in security of employment network,” Jun. 01, 2012. doi: 10.1109/isra.2012.6219267.

[30] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, “A Survey on Honeypot Software and Data Analysis,” Jan. 01, 2016, Cornell University. doi: 10.48550/arxiv.1608.06249.

[31] Educational Institutions Data Breaches in India - An Analysis: https://www.linkedin.com/pulse/educational-institutions-data-breaches-india-analysis-nk5df/